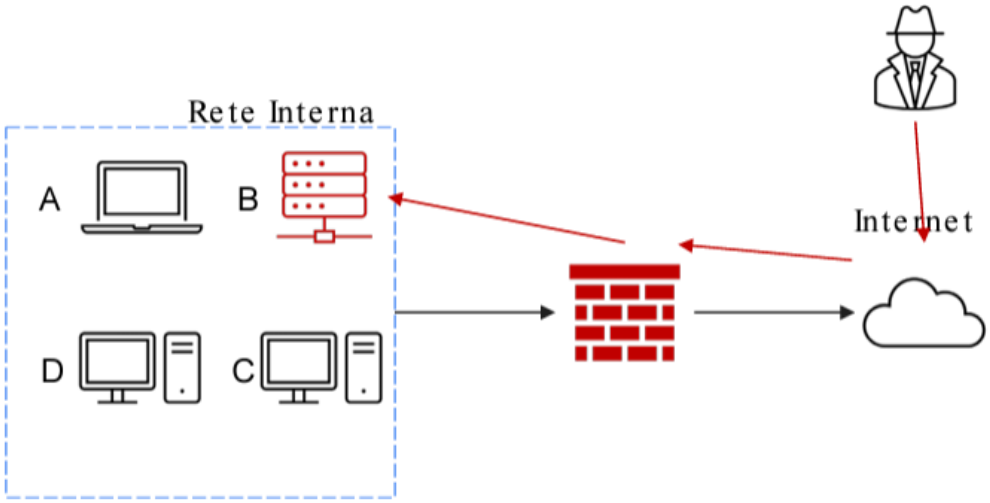
S9L4 - ESERCIZIO TECNICHE ISOLAMENTO



Traccia

Con riferimento alla figura in alto, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti:

- Mostrate le tecniche di:
  - Isolamento
  - Rimozione del sistema B infetto

- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.
- Indicare anche Clear

Svolgimento

Tecniche di Isolamento

Isolamento della Rete:

- **Disconnessione Immediata:** Disconnettere immediatamente il sistema compromesso (Sistema B) dalla rete. Questo può essere fatto rimuovendo il cavo di rete o disabilitando l'interfaccia di rete, impedendo ulteriori esfiltrazioni di dati e bloccando l'accesso dell'attaccante ad altre parti della rete.
- **Aggiornamento delle Regole del Firewall:** Modificare le regole del firewall per bloccare tutto il traffico in entrata e in uscita dall'indirizzo IP del Sistema B. Questo assicura che il sistema non possa comunicare con altri sistemi della rete o con Internet.
- **Segmentazione:** Se non già implementata, segmentare la rete per isolare i sistemi critici gli uni dagli altri. Questo limita la diffusione dell'attacco e protegge altri sistemi (A, C, D) nella rete.

Isolamento Fisico:

- **Disconnessione Fisica:** Rimuovere fisicamente i dispositivi di archiviazione dal Sistema B per prevenire ulteriori accessi non autorizzati.
- **Restrizione degli Accessi:** Limitare l'accesso fisico all'hardware solo al personale autorizzato, assicurandosi che nessuna persona non autorizzata possa manomettere il sistema.

Rimozione del Sistema Infetto

Rimozione del Sistema B:

- **Backup dei Dati:** Se possibile, effettuare un backup forense del sistema compromesso prima di apportare qualsiasi modifica. Questo backup è cruciale per l'analisi dell'incidente e per adottare misure preventive future.
- **Spegnimento:** Spegnere il sistema in modo sicuro per evitare la corruzione dei dati.
- **Analisi Forense:** Prima di riformattare o smaltire qualsiasi hardware, dovrebbe essere condotta una dettagliata analisi forense per comprendere la natura e la portata della violazione. Questa analisi è utile per prevenire attacchi futuri.

Sanitizzazione dei Dati: Clear, Purge e Destroy

Clear, Purge e Destroy sono metodi per la sanitizzazione dei supporti di archiviazione:

- **Clear (Pulizia):**
    - **Definizione:** La pulizia comporta la sovrascrittura dello spazio di archiviazione con dati non sensibili (zeri o dati casuali) per rendere più difficile il recupero dei dati originali.
    - **Caso d'Uso:** Questo metodo è adatto per scenari in cui i supporti saranno riutilizzati all'interno dell'organizzazione. Riduce la probabilità di recupero dei

dati, ma non garantisce che i dati non possano essere recuperati con metodi sofisticati.

- **Purge (Purgare):**
    - **Definizione:** La purga rende il recupero dei dati inattuabile anche con tecniche avanzate. Questo metodo è più rigoroso rispetto al clearing e spesso comporta la rimozione fisica di strati del disco o l'applicazione di metodi di sovrascrittura multipli.
    - **Caso d'Uso:** È utilizzato quando i dispositivi devono essere trasferiti fuori dall'organizzazione o quando c'è un rischio elevato di accesso non autorizzato.
- **Destroy (Distruzione):**
    - **Definizione:** La distruzione comporta il danneggiamento fisico irreversibile dei supporti, rendendo i dati completamente irrecuperabili.
    - **Caso d'Uso:** Utilizzata quando è necessario eliminare permanentemente le informazioni sensibili e non è previsto alcun riutilizzo dei supporti.

In sintesi, la scelta tra **Clear**, **Purge** e **Destroy** dipende dal livello di sensibilità dei dati e dalla necessità di sicurezza nel garantire che i dati non possano essere recuperati.